Computing Policy

Version 2.1
Date 03/11/10

INTRODUCTION

The following is a list of general computer use policies and security rules that apply to all users of the Oak Ridge Leadership Computing Facility (OLCF) resources. Principal investigators are responsible for implementing these policies and procedures in their organizations and ensuring that users fulfill their responsibilities.

COMPUTER USE

Computers, software, and communications systems provided by the OLCF are to be used for work associated with and within the scope of the approved project. All computers, networks, E-mail, and storage systems are property of the United States Government. Any misuse or unauthorized access is prohibited, and is subject to criminal and civil penalties.

OLCF systems are provided to our users without any warranty. OLCF will not be held liable in the event of any system failure or data loss or corruption for any reason including, but not limited to: negligence, malicious action, accidental loss, software errors, hardware failures, network losses, or inadequate configuration of any computing resource or ancillary system.

DATA USE

Prohibited Data

The OLCF computer systems are operated as research systems and only contain data related to scientific research and do not contain personally identifiable information (data that falls under the Privacy Act of 1974 5U.S.C. 552a). Use of OLCF resources to store, manipulate, or remotely access any national security information is strictly prohibited. This includes, but is not limited to: classified information, unclassified controlled nuclear information (UCNI), naval nuclear propulsion information (NNPI), the design or development of nuclear, biological, or chemical weapons or any weapons of mass destruction. The use of OLCF resources for personal or non-work-related activities is also prohibited.

Authors/generators/owners of information are responsible for its correct categorization as sensitive or non-sensitive. Owners of sensitive information are responsible for its secure handling, transmission, processing, storage, and disposal on OLCF systems.

Principal investigators, users, or project delegates that use OLCF resources, or are responsible for overseeing projects that use OLCF resources, are strictly responsible for knowing whether their project generates any of these prohibited data types or information that falls under Export Control. For questions, contact help@nccs.gov.

Confidentiality, Integrity, and Availability

The OLCF systems provide protections to maintain the confidentiality, integrity, and availability of user data. Measures include the availability of file permissions, archival systems with access control lists, and parity and CRC checks on data paths and files. It is the user’s responsibility to set access controls appropriately for the data. In the event of system failure or malicious actions, the OLCF makes no guarantee against loss of data or that a user’s data can be accessed, changed, or deleted by another individual. It is the user’s responsibility to insure the appropriate level of backup and integrity checks on critical data and programs.

Data Modification/Destruction

Users are prohibited from taking unauthorized actions to intentionally modify or delete information or programs.

Data Retention

The OLCF reserves the right to remove any data at any time and/or transfer data to other users working on the same or similar project once a user account is deleted or a person no longer has a business association with the OLCF.

After a sensitive project has ended or has been terminated, all data related to the project must be purged from all OLCF computing resources within 30 days.

SOFTWARE USE

All software used on OLCF computers must be appropriately acquired and used according to the appropriate software license agreement. Possession, use, or transmission of illegally obtained software is prohibited. Likewise, users shall not copy, store, or transfer copyrighted software, except as permitted by the owner of the copyright. Only export-controlled codes approved by the Export Control Office may be run by parties with sensitive data agreements.

Malicious Software

Users must not intentionally introduce or use malicious software such as computer viruses, Trojan horses, or worms.

Reconstruction of Information or Software

Users are not allowed to reconstruct information or software for which they are not authorized. This includes but is not limited to any reverse engineering of copyrighted software or firmware present on OLCF computing resources.

USER ACCOUNTABILITY

Users are accountable for their actions and may be held accountable to applicable administrative or legal sanctions.

Monitoring and Privacy

Users are advised that there is no expectation of privacy of your activities on any system that is owned by, leased or operated by UT-Battelle on behalf of the U.S. Department of Energy (DOE). The Company retains the right to monitor all activities on these systems, to access any computer files or electronic mail messages, and to disclose all or part of information gained to authorized individuals or investigative agencies, all without prior notice to, or consent from, any user, sender, or addressee. This access to information or a system by an authorized individual or investigative agency is in effect during the period of your access to information on a DOE computer and for a period of three years thereafter.

OLCF personnel and users are required to address, safeguard against, and report misuse, abuse and criminal activities. Misuse of OLCF resources can lead to temporary or permanent disabling of accounts, loss of DOE allocations, and administrative or legal actions.

Users who have not accessed a OLCF computing resource in at least 6 months will be disabled. They will need to reapply to regain access to their account. All users must reapply annually.

Authentication and Authorization

All users are required to use a one-time password for authentication. Tokens will be distributed to OLCF users. Users will be required to create a Personal Identification Number (PIN). This is used in conjunction with a generated token code as part of a two-factor authentication implementation.

Computing Policies Ver 2.1

Accounts on the OLCF machines are for the exclusive use of the individual user named in the account application. Users should not share accounts or tokens with anyone. If evidence is found that more than one person is using an account, that account will be disabled immediately.

Users are not to attempt to receive unintended messages or access information by some unauthorized means, such as imitating another system, impersonating another user or other person, misuse of legal user credentials (usernames, tokens, etc.), or by causing some system component to function incorrectly.

Users are prohibited from changing or circumventing access controls to allow themselves or others to perform actions outside their authorized privileges.

Users must notify the OLCF immediately when they become aware that any of the accounts used to access OLCF have been compromised.

Users should inform the OLCF promptly of any changes in their contact information (E-mail, phone, affiliation, etc.) Updates should be sent to accounts@ccs.ornl.gov.

Foreign National Access

Applicants who appear on a restricted foreign country listing in section 15 CFR 740.7 License Exceptions for Computers are denied access based on US Foreign Policy. The countries cited are Cuba, Iran, North Korea, Sudan, and Syria. Additionally, no work may be performed on OLCF computers on behalf of foreign nationals from these countries.

Denial of Service

Users may not deliberately interfere with other users accessing system resources.

Computing Policies Vsn 2.1